STATEMENT

OF

LAUREN B. STEINFELD

Formerly Associate Chief Counselor for Privacy at the Office of Management and Budget
Currently, Chief Privacy Officer, University of Pennsylvania

BEFORE THE

SUBCOMMITTEE ON

COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE

UNITED STATES HOUSE OF REPRESENTATIVES

Social Security Numbers in Commerce – Reconciling Beneficial Uses with Threats to Privacy

May 11, 2006

Good morning and thank you for the opportunity to speak before you today about Social Security Numbers in Commerce – Reconciling Beneficial Uses with Threats to Privacy. I am delighted to share some views on an issue about which I have thought for some time. In today's testimony, I will describe some examples of the risks and benefits of using SSNs. I will also share my view that the two bills being considered by this Committee, H.R. 1078 and H.R. 1745, go far towards advancing privacy protection while also addressing important commercial, health, and safety concerns. Finally, I will offer some views on particular provisions in the bills.

My background on privacy issues is as follows. I began working at the Federal Trade Commission in 1995 where I was a staff attorney in the Division of Financial Practices and then in 1998 served as Attorney Advisor to Commissioner Mozelle Thompson. The following year, I became Associate Chief Counselor for Privacy, working for Peter Swire, the Chief Counselor for Privacy, at the Office of Management and Budget. In this role, I worked on a wide variety of privacy issues, two of which are especially relevant to this discussion: First, I served as the lead staff person to help develop proposed legislation regarding Social Security number protection – the Social Security Number Protection Act of 2000 was introduced by Representative Markey as H.R. 4611 and Senator Feinstein as S. 2699. Second, I was the coordinator within OMB for the report issued by OMB, the Department of Treasury and the Department of Justice entitled "Financial Privacy in Bankruptcy: A Case Study on Privacy in Public and Judicial Records." Currently, I serve as Chief Privacy Officer for the University of Pennsylvania where I coordinate programs on a number of fronts to reduce SSN-related risks.

In today's testimony, I am presenting my own views based on my experiences and not the views of the University of Pennsylvania, nor the views of the Clinton or Bush Administrations from my time at OMB.

The Risks and Benefits of SSNs

We, as a society, are struggling to get our arms around how to manage a small piece of data that can raise big problems and provide big benefits – that is, the Social Security number. The most common problem the SSN creates is that it can be used, indeed abused, by thieves, in combination with often other publicly available data, to commit identity theft. Often identity theft occurs in the following way: the thief starts by obtaining a limited amount of information about someone else and uses it to obtain credit, for example by opening a credit card account or cell phone account, in the victim's name. The thief then runs up charges on the account and fails to pay those charges. The victim's credit reports will show significant delinquencies that interfere with the victim's ability to obtain a loan, a mortgage, insurance, even a job. In addition to damage to identity theft victims, identity theft also costs credit providers who are not paid amounts based on fraudulent charges. These costs are eventually largely borne by honest users of credit who pay more.

Another example of identity theft comes in the context of tax filings. A thief may use a legitimate taxpayer's personal information to file a fraudulent tax return designed to provide a refund. Those thieves may then go on to take out "refund anticipation loans," based on the amount they have "allowed themselves" in their filing. A recent New York Times article, based on an interview with an IRS official, reported that there were 8,000 instances in one year of information of legitimate taxpayers being used by imposters to try to defraud the tax system.

Identity theft is now the fastest growing crime in America, because of the ease with which it can be committed. It is so easy because the very limited information required to open accounts is easily available. While name and address and even date of birth are often presumed to be public, it is the Social Security number that is intended to be the one key piece of private data that lets, for example, creditors know they are in fact extending credit to the person whom the applicant claims to be. When that Social Security number is not in fact private, a key foundation for the integrity of the credit granting system is compromised. I have heard anecdotally from a law enforcement officer that in the past, the conversation in prison yards centered on bank robbery. Now, the "buzz" is that bank robbery is too difficult; identity theft is the way to go.

It is tempting as a society to declare then that Social Security numbers should be banned except for purposes of administering the Social Security system and for tax-related purposes. But to shut down the use of Social Security numbers poses different, but also highly significant, problems.

Social Security numbers are the closest thing we have to a national identifier and, by helping to link different data sources, they are often the key to advancing national priorities. They facilitate important commercial activities, including the granting of loans, insurance and employment through the credit reporting system that – when working ideally – allows industry to judge an applicant according to information *about that applicant.* They help us gather critical public health data for investigations and sometimes life-saving interventions. They enable vital health-related research on individuals over time and over different health care settings. Social Security numbers help us locate missing children and fugitives from justice and generally provide crucial data for law enforcement and national security purposes.

Crafting Legislation

With the risks and the benefits of Social Security numbers largely understood, the challenge in crafting legislation is how best to tackle the privacy concerns, without creating the unintended consequences of hindering fraud detection, law enforcement, national security, research, and other significant priorities. In my personal opinion, the two bills being considered by the Committee strike the balance quite well in many respects.

Banning the Uncontrolled Sale and Purchase of SSNs

First and foremost, the bills would outlaw the uncontrolled sale and purchase of Social Security numbers. Today, it is lawful to create a website and offer SSNs for sale – regardless of who is asking and regardless of the purpose. In fact, one website I found advertises “Locate a Social Security number -- Supply a name & address or previous address, we will supply a social security number!” Another site says,

> “The Internet is the largest information base in the world, and we have uncovered thousands of resources that will have you simply amazed ... and all of this is 100% legal.”

When working on SSN-related initiatives at the University of Pennsylvania, I have heard people remark that while we are spending great amounts of money, time, and effort to remove SSNs from our systems and documents, and to convert to what we call a “PennID,” it is frustrating to know that the SSNs we are protecting are literally “for sale” by others on the Internet. Legislation banning the uncontrolled sale or purchase of SSNs can help send a strong signal to organizations working to protect SSNs that their efforts are even that much more worthwhile.

As I stated above, the bills would outlaw the *uncontrolled* sale and purchase– but not *all* sales and purchases. That is appropriate to accommodate the critical beneficial uses of SSNs described above. Both H.R. 1078 and H.R. 1745 set out largely similar exceptions to the restrictions on the sale and purchase of SSNs. They allow, for example, SSNs to be sold or purchased for law enforcement or national security purposes, for public health purposes, for emergency situations, to the extent necessary for research, and pursuant to consent – and each bill allows for further development of the exceptions in a subsequent rulemaking.

Differences in Approach to Rulemaking

A key difference in the bills lies in how that rulemaking will be conducted. H.R. 1078 gives the Federal Trade Commission authority to promulgate rules within one year regarding unfair or deceptive acts or practices in connection with the sale and purchase of SSNs – all in consultation with the Commissioner of Social Security, the Attorney General, and other agencies as the Commission deems appropriate. H.R. 1745 gives the rulemaking authority to the Attorney General, in consultation with the Commissioner of Social Security, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Secretary of the Treasury, the Federal Trade Commission, the Federal banking agencies, and National Credit Union Administration, the Securities and Exchange Commission, State attorneys general, and certain State insurance commissioners.

In my opinion, the Federal Trade Commission should be given the primary authority to issue regulations in this area for the following reasons:

- The FTC has significant expertise in understanding identity theft through the program it administers under the Identity Theft Assumption and Deterrence Act of 1998. In particular, the FTC is well versed on the causes of identity theft and is in a solid position to address the privacy risks in overexposing SSNs.
- The FTC also has a deep understanding of the competing interests to SSN restriction through its work with the data broker industry, first in helping to develop the industry self-regulatory program in the late 1990s and more recently in the aftermath of the Choicepoint breach.
- Finally, the FTC, through its experience in promulgating the Safeguards Rule under the Gramm-Leach-Bliley Act, is aware of the important difference between "reasonable

> safeguards" and "perfect security." As a result, the FTC has now developed more technical expertise to evaluate burdens and benefits in securing the sensitive SSN.

While I believe the FTC expertise should be leveraged to the fullest advantage, I also believe that consultation with the agencies named in H.R. 1745 would provide additional controls to ensure that the many considerations of beneficial and risky uses are addressed.

As far as what the rulemaking should cover, I recommend that the bills contain an additional provision – the rulemaking agency should address the issue of verifying the identity and authority of requesters seeking SSNs under one of the enumerated exceptions. We have seen in the Choicepoint breach that a critical control to protecting privacy is adopting robust procedures to check the credentials of callers and writers claiming to be legitimate and to be using data for legitimate purposes. Today, certain websites are willing to furnish sensitive data such as Social Security number on the mere "I agree" click that I have a permissible purpose under the Fair Credit Reporting Act. It is worth considering the burdens and benefits of different verification approaches to provide reasonable assurances that requests truly are legitimate. Adding requirements in this area is important to realize the goals of the bills overall.

Additional Regulation in H.R. 1745

Another key difference between H.R. 1078 and H.R. 1745 is that the latter goes beyond restricting the sale and purchase of SSNs. H.R. 1745 reaches into many additional areas that are well worth acting upon and for the most part do not raise the same types of tradeoffs. The provisions dealing with public display of SSNs are especially valuable.

H.R. 1745 places special provisions on governmental agencies and prohibits them from displaying SSNs on checks issued for payment. For the public and private sector, the bill also prohibits placing SSNs on employee identification cards or tags. H.R. 1745 also prohibits inmate access to SSNs. These measures are entirely appropriate as a risk benefit matter, though one must recognize that even seemingly simple process changes, when applied so broadly, can take significant time and resources. I encourage the Committee to confirm the appropriate timeframe for instituting these measures.

H.R. 1745 also includes a requirement that both the public and the private sector adopt "measures to preclude the unauthorized disclosure of Social Security numbers." The spirit of this provision seems very well aligned with the Safeguards Rule of the Gramm-Leach-Bliley Act. I encourage aligning the language of the bill more closely with the GLB Safeguards Rule and, again, vesting rulemaking authority with the Federal Trade Commission to help achieve that consistency.

One final point on H.R. 1745 concerns Section 109 – making it unlawful to refuse to do business with an individual because the individual will not provide a Social Security number – that provision being effective within 180 days. I suspect that this provision could be very problematic for some industries in this time frame, particularly health care, where the SSN may very well be the key to linking medical data for treatment purposes, coordinating benefits, and performing critical medical research. I encourage the Committee to review this provision and the timeframe more closely and to reach out to affected industries, before passing legislation. Alternatively, the impact of this provision could be researched and the language refined in a rulemaking as well.

Conclusion

There is ample room for optimism in greatly reducing risks arising from the overavailability of Social Security numbers. This is a critical effort and will remain so for as long as we have credit processes that allow for the extension of credit based on name, address, and Social Security number alone.

In the last several years, we have learned a great deal about workable models for protecting privacy without compromising important other priorities. For example, I described above the work of OMB, the Department of Treasury and the Department of Justice on "Financial Privacy in Bankruptcy: A Case Study on Privacy In Public and Judicial Records." That report recommended what I believe to be a balanced model in which full bankruptcy case files are available to "real parties in interest," to enable them to protect their rights, while the general public would be restricted from certain sensitive data, like Social Security numbers and bank account numbers, that are not necessary for the public to know in the name of accountability of the bankruptcy system. In this example, combined with many others, we have learned that privacy and accountability – or commerce or national security as the case may be -- may be spoken in the same sentence and often do one another a service. When stakeholders from all vantage points work in earnest on crafting a better data confidentiality model – all are better off.

My optimism is confirmed by the authors of the two bills before the Committee who recognize that the time has come for a consensus to prohibit the uncontrolled sale and purchase of the highly sensitive Social Security number. I am pleased that the authors are finding ways to take important steps to protect privacy while also protecting other critical goals. I thank you for the opportunity to appear before you and welcome any questions you may have.